DIRECTOR-GENERAL'S ANNUAL THREAT ASSESSMENT

Good evening. Welcome to ASIO and to my Annual Threat Assessment.

I'd like to recognise our partners and colleagues represented here tonight – Excellencies, MP's and Senators, the Inspector-General, Directors-General, Secretaries, Military Chiefs, Commissioners, ladies and gentlemen.

Can I start with an admission? While I am pleased to host this event and welcome you to the Ben Chifley Building, a lectern is not my happy place. I loathe public speaking.

So you might be thinking, why would someone like me choose to do something like this?

There are three key reasons, and I'd like to explain them.

The first is trust.

ASIO protects Australia and Australians from threats to their security. Our ability to deliver our mission requires us to maintain the confidence and trust of our stakeholders, including the Australian people.

A vibrant liberal democracy requires a Security Service that is transparent and trusted.

I believe this imposes a responsibility on ASIO to be as open as possible about what the Organisation does, and why we do it.

Giving this address, and inviting you into our building, is a tangible expression of how seriously I take that responsibility.

It's why I was one of the first intelligence leaders anywhere in the world to have a personal, identifiable Twitter account; why I give speeches and do occasional media interviews; why ASIO is on social media; and why I've declassified operations and case studies to give a clearer picture of the threats we face.

None of that was easy. Some of it was controversial. But all of it was important.

Transparency matters. Transparency is a precursor for trust.

My thinking on transparency crystallised at a time in my career when the Defence Signals Directorate was accused of an illegal act.

The allegations were proved to be completely unfounded, but damage was done, reputations were stained, and confidence was bruised.

The affair taught me how difficult it can be for a secret organisation to defend itself, even when it's done nothing wrong—it's assumed that if you're in the shadows, you're shadowy.

We can dispel this with sunlight—by explaining who we are, what we do, and why we matter.

Not long after that incident, a journalist put a salacious and inaccurate claim to a certain intelligence agency—I won't say which one, or even in which country. Instead of saying, 'that's ridiculous'—or 'hell no', which would have been my response—the brains trust replied with, 'no comment—and that's off the record'.

The story got published and the next morning there was much head-shaking and tut-tutting as spy chiefs wondered how the newspaper could get it so wrong. The journalist got it so wrong because the agency ignored an opportunity to make it right!

Obviously there are things a spy agency cannot talk about—especially one where human sources and technical capabilities are critical to its success.

We need to be able to do things our adversaries think are impossible. But as I rose through the ranks, it became increasingly clear that there is much more we can say than 'no comment'.

We don't talk about our operations but we can reveal their outcomes.

We must be secretive about our capabilities, but we can be open about our values.

We cannot identify our undeclared staff, but we can celebrate the difference they make.

That brings me to the second principle of my transparency push— ASIO's people. Transparency is a powerful recruitment tool. People won't work for an agency if they don't know what it does and what it values; they can't apply for jobs they don't know exist.

I want more people to choose ASIO, and I want ASIO to be able to choose more people from more diverse backgrounds. This is a challenge intelligence agencies around the world are grappling with.

We need to do better. We should reflect the community we protect.

It's never too early to start planning a career at ASIO.

I recently received a letter from seven-year-old Ava, who wants to be a surveillance officer. She told me she's good at spying because she is small and nobody notices her.

Ava volunteered her mum to drive her around on her surveillance shifts. Clearly, young Ava already possesses some of the skills we're looking for—she's creative, shows initiative, and can communicate. But hide-and-seek isn't just for kids, and surveillance isn't just hide and seek. We are actually hiring surveillance officers right now.

While surveillance is a traditional spy role, we have many other roles too. Many of the jobs we are advertising, or are about to advertise, are not usually associated with spy agencies, but are integral to our success:

- Trades professionals such as electricians and plumbers.
- Technology graduates who can design, build and deliver systems, access data and help our analysts make sense of data.
- Business analysts and project managers to drive our capability uplift.
- Intelligence officers and analysts to collect the dots and connect the dots.
- And legal graduates to ensure our covert operations are conducted lawfully, and to work on litigation and corporate matters.

There is no ASIO type. ASIO needs people from all walks of life and I invite you to find your fit.

So that's what an annual threat assessment delivers for ASIO.

The final—and perhaps most important—factor is what's in it for you, ASIO's partners and stakeholders. It's critically important to explain the threats we are seeing so you are armed with the awareness and advice you need to counter those threats.

Security is a shared responsibility. ASIO cannot stop every terrorist and catch every spy. The scale, persistence and sophistication of the threats Australia is facing demands a broader approach to security. I'll return to this later.

Australia's security outlook remains complex, challenging and changing. COVID-19 and its associated lockdowns added considerable volatility to the mix.

While, thankfully, the time of lockdowns seems to have come to an end, the impacts of the lockdowns are continuing to influence the security environment.

We all spent a lot more time online during the pandemic. This was positive in many respects. During difficult times, the internet helped us maintain connections with families and friends, allowed many of you to work from home, and, of course, enabled plenty of online shopping!

But like many things online, for every benefit the internet delivered, a related downside was created.

More online shopping meant more cyber-crime. More online engagement provided greater opportunities for radicalisation. More working from home increased the risk of cyber-enabled espionage.

I'd like to dive into the last two a little more deeply because they fall squarely within ASIO's remit, and are exerting a significant influence on Australia's security environment.

In the last two years, thousands of Australians with access to sensitive information have been targeted by foreign spies using social media profiles. These spies are adept at using the internet for their recruitment efforts.

On any of the popular social media or internet platforms, they make seemingly innocuous approaches—such as job offers. This then progresses to direct messaging on different, encrypted platforms, or in-person meetings, before a recruitment pitch is made.

I've previously highlighted our concerns about approaches on professional networking sites, but during the pandemic we've seen this threat spread. There's been a jump in suspicious approaches on messaging platforms like WhatsApp, for example.

It's an easy way for foreign intelligence services to target employees of interest.

ASIO is also tracking suspicious approaches on dating platforms such as Tinder, Bumble and Hinge. My message for any potential victims on these sites is a familiar one—if it seems too good to be true, it probably is!

While espionage is one of the most insidious security threats we are dealing with online, it is not the most concerning trend.

The internet is the world's single most potent and powerful incubator of extremism.

Online radicalisation is nothing new, but COVID-19 sent it into overdrive. Isolated individuals spent more time online, exposed to extremist messaging, misinformation and conspiracy theories.

Social media platforms, chat rooms, and algorithms are designed to join up people who share the same views, and push them material they will 'like'. It's like being in an echo chamber where the echo gets louder and louder, generating cycles of exposure and reinforcement.

More time in those online environments—without some of the circuit breakers of everyday life, like family and community engagement, school and work—created more extremists. And in some cases, it accelerated extremists' progression on the radicalisation pathway towards violence.

Back in 2007, ASIO produced an assessment warning about the implications of a pandemic. We did that not because we're health experts, but because it's our job to identify and analyse phenomena that might have security impacts for our country. We assessed that a pandemic would result in an increase in anti-government behaviours, and we have certainly seen that with COVID.

While ASIO's overall terrorism caseload has decreased since this time last year, there's been a distinct increase in radicalisation and specific-issue grievances.

Some Australians believe the government's approach to vaccinations and lockdowns infringed their freedoms. And in a small number of cases, grievance turned to violence.

Obvious examples are the violent incidents at COVID-related protests fuelled by anti-vaccination, anti-lockdown and anti-government agendas.

We have also seen threats against public office holders, an attack on a vaccination clinic, and several physical assaults on healthcare workers.

We assess that these tensions and the associated possibility of violence will persist.

While lockdowns and mandatory quarantine requirements are being eased, the introduction of vaccination requirements for some forms of employment, social engagement and travel will continue to drive anger, uncertainty and fear within a small section of society.

This cohort views the restrictions as an attack on their rights, the creation of a two-tier society and confirmation of their perceived persecution.

ASIO does not have any issue with people who have opinions they want to express. This is a critical part of a vibrant democracy. We do not—and cannot—investigate peaceful protest or dissent. Our concern is where opinions tip into the promotion of violence, or actual acts of violence.

So I should stress that the vast majority of people who choose not to be vaccinated will not engage in violence in response to vaccine mandates. The vast majority of protestors are not violent extremists, and the vast majority of the protests are not violent. ASIO's focus is on a small number of angry and alienated Australians.

This is precisely the concern I identified in this speech last year, and precisely why we changed the language we use to describe violent extremism. As I warned back then:

We are seeing a growing number of individuals and groups that don't fit on the left–right spectrum at all; instead, they're motivated by a fear of societal collapse or a specific social or economic grievance or conspiracy.

The behaviours we are seeing in response to COVID lockdowns and vaccinations are not specifically left or right wing. They are a cocktail of views, fears, frustrations and conspiracies. Individuals who hold these views, and are willing to support violence to further them, are best and most accurately described as ideologically motivated violent extremists.

Some of the alleged violent acts at the recent Old Parliament House protest are a case in point. The individuals involved were driven by a diverse range of grievances, including anti-vaccination agendas, conspiracy theories and anti-government sovereign citizen beliefs.

Assigning the protesters to a specific point on the political spectrum is neither accurate nor helpful.

Of course, this does not mean that people who hold, say, racist and nationalist beliefs never participate in these activities—sometimes they do—but they are just one relatively small part of a much wider and looser group.

This is an important point to make, because we expect to see more of this behaviour in Australia in the medium term. Protests driven by diverse specific-issue grievances will be part of our security environment for the foreseeable future. In some cases, protesters will advocate the use of violence, and in a smaller number of cases, they may use violence.

In this uptick in specific-issue or grievance-motivated violent extremism, many of the actors are newcomers, so it's harder to get a sense of what is simply big talk—and what is genuine planning for violence.

Making the call about which statements indicate a genuine plan for violence, and which are purely sounding off or wishful thinking, is one of the greatest challenges our analysts have. Our information is often incomplete—and the stakes are high.

Every judgement our analysts make affects another: when they decide to continue one investigation they are, in effect, deciding not to continue or launch a different one. With finite resources, it is a zero-sum game.

The most likely terrorist attack scenario in Australia over the next 12 months continues to be a lone-actor attack—and that fact weighs heavily on my mind and the minds of our staff.

While there were no terrorist attacks domestically last year, there were two major disruptions of violent extremist attacks. Globally, violent extremist attacks remain a frequent occurrence. And the transnational nature of terrorism means that events in distant places, such as the fall of the government in Afghanistan, can reverberate much closer to home. We are monitoring this carefully.

While we do not assess it has increased the immediate threat in Australia, we remain concerned that, in the longer term, violent extremists from our region may travel to Afghanistan for militant training.

Two years ago, in my first threat assessment, I noted that ASIO was seeing an increase in the radicalisation of young Australians.

Unfortunately and alarmingly, this trend is continuing. The number of minors being radicalised is getting *higher* and the age of the minors being radicalised is getting *lower*.

Most of the radicalisation occurs online, reflecting the dynamic I raised earlier, but some of it also happens in person, face to face. Children as young as 13 are now embracing extremism, and this is happening with religiously motivated violent extremism and ideologically motivated violent extremism.

And unlike past experience, many of these young people do not come from families where a parent or sibling already holds extreme views.

As the Director-General of Security, this trend is deeply concerning. As a parent, it is deeply distressing. As a nation, we need to reflect on why some teenagers are hanging Nazi flags and portraits of the Christchurch killer on their bedroom walls, and why others are sharing beheading videos. And just as importantly, we must reflect on what we can do about it.

A few years ago, minors represented around two to three per cent of our new counter-terrorism investigations. In the last year, though, the figure's been closer to *fifteen* per cent. And perhaps more disturbingly, these young people are more intense in their extremism.

Where once minors tended to be on the fringe of extremist groups, we are now seeing teenagers in leadership positions, directing adults, and willing to take violent action themselves.

At the end of last year, on average, minors represented more than half of our priority counter-terrorism investigations each week.

This should concern us all. Again, minors made up 15 per cent of our new counter-terrorism investigations, and more than half of our highest priority investigations each week.

ASIO is aware of minors preying on other minors, seeking to turn them to their violent ideology and using grooming techniques similar to those used by paedophiles.

We have seen cases involving young, radicalised violent extremists systematically targeting vulnerable associates who were lonely or going through tough times.

The targeting took place online, and face to face in a variety of settings, even schools. The tactics used by the extremists in these cases involved a combination of attention, flattery and friendship, which shifted to bullying and manipulation. We've seen young ringleaders deliberately desensitise their targets, gradually exposing them to more extreme and more violent propaganda, until the most graphic material imaginable was normalised.

Believe me when I tell you that ASIO finds these kinds of cases challenging—we do not belong in the schoolyard—and while we act when there is a threat of violence, the broader trend of teenage radicalisation demands a different response, one where ASIO and law enforcement are not the answer.

It is very hard to deradicalise an adult extremist, but there are many more options to redirect young people who are experimenting with extremism in response to unhappiness or insecurity.

As a society, we have to recognise the signs and step in early. Radicalisation in young people can happen quickly—in days and weeks, not months and years—and kids are most vulnerable when they are under stress.

In these situations, ASIO's role is at the end—at the point where there is an active threat to security. But before this point there are nearly always off-ramps: opportunities to redirect behaviour.

Government plays a key role in helping to counter violent extremism. Our colleagues in policy agencies, law enforcement and community organisations are doing important work in this space.

But the community can play a pivotal part identifying signs a teenager isn't just going through adolescence, but is heading towards radicalisation. Without knowing about these indicators it is much harder for us to divert them from a dangerous path.

Schools and sports clubs—notice and ask questions if the young people you know are acting antisocially and out of character.

Parents and carers—notice and ask questions if your children are receiving or circulating inappropriate material online. Children often start with moderately objectionable material, which then becomes worse and worse—identifying it early can be critical.

Community leaders—notice and ask questions if young people you know are showing marked changes in their demeanour or views.

Security is a shared responsibility.

While threat to life will always be a priority for ASIO, our attention and resourcing is increasingly being directed towards threats to Australia's way of life.

The first and perhaps most significant thing to say is that espionage and foreign interference has supplanted terrorism as our principal security concern.

This is not to downplay the significance of terrorism.

In terms of scale and sophistication, though, espionage and foreign interference threats are outpacing terrorism threats, and therefore demanding more attention and more resources.

The threat is pervasive, multifaceted and, if left unchecked, could do serious damage to our sovereignty, values and national interest.

Multiple countries are seeking to conduct espionage against us—and not just those countries that might be considered our traditional adversaries. In some instances, espionage is conducted by countries we consider friends—friends with sharp elbows and voracious intelligence requirements.

For decades, foreign spies have been seeking information about Australia's strategic capabilities, economic and policy priorities, world-class research and development, and defence technologies.

Obviously the capabilities and decision-making around AUKUS fall squarely into that category. Foreign intelligence agencies will have already added them to their collection requirements—just as ASIO is already working to thwart them. That should surprise no one; it's one of the reasons I'm flagging a more proactive approach to our security advice and engagement.

Following my previous address, our disruption of a 'nest of spies' got a lot of attention. But dismantling spy networks is business as usual for ASIO. We did it again last year.

Over a series of months, we painstakingly mapped out a foreign intelligence service's onshore network of sources and contacts. And then we picked it apart.

Australians who were targeted by the foreign intelligence service included current and former high-ranking government officials, academics, members of think-tanks, business executives and members of a diaspora community.

When we interviewed members of the network, some of the contacts suspected they'd engaged with spies, but most had no idea—and were shocked when we knocked on their doors.

As a sting in the tail, after we removed the spies, we laid trip wires—just in case the foreign country ever tries to reactivate this network. And this was just one of a number of disruptions we undertook in the past year.

As well as espionage, we've also seen an increase in foreign interference. I want to take a moment to draw out how this is different from foreign influence.

The confusion about where legitimate influence stops and foreign interference begins is understandable. We see our targets engaging in both things, and foreign interference is clandestine, and therefore difficult to discern.

Publicly praising a foreign regime—even an odious one—is not interference.

Transparently lobbying on behalf of a foreign government is not interference.

Diplomacy is not interference. These things are routine acts of statecraft.

But any and all of these acts could become foreign interference if they involve the hidden hand of a foreign state and are contrary to Australia's interests. If the person publicly praising another country is doing so because they've received discreet instructions from an overseas government, it could constitute foreign interference if it's detrimental to Australia's interests or done to affect our political processes.

So what does foreign interference look like in practice? There are two manifestations I'd like to focus on.

One is the harassment of Australia's diaspora communities. This is something ASIO's been warning about for some time. Foreign governments will often monitor and intimidate members of diaspora communities who are critics of the foreign government or express views at odds with the regime's policies. It's unacceptable that people who live in your street—and mine—might be subjected to the strongarm—and long arm—of a foreign state.

Again, it's important to understand exactly what is, and is not, foreign interference in this context. Just as it is perfectly legal to criticise a foreign regime in this country, it is perfectly legal to stage a counter-protest. That is not necessarily foreign interference, it may just be nationalist zeal.

But if a foreign government is clandestinely directing the counter-protest, then my Organisation will be very interested.

Some of the foreign governments we've dealt with seem to think that this sort of community harassment is OK. They think wrong. It's not OK.

One of the most insidious things about foreign interference is that it uses our strengths against us. The perpetrators exploit our values, freedoms and trust, to undermine our values, freedoms and trust.

Foreign interference in our politics is a case in point. The government**s**—and I emphasise government**s**—involved in these activities take advantage of the open and accessible nature of our political system.

Attempts at political interference are not confined to one side of politics, and you'd be surprised by the range of countries involved.

It's also important to put it in context. While attempts to interfere in our democratic processes are common, successful interference is not.

Our democracy remains robust, our parliaments remain sovereign, our elections remain free and the overwhelming majority of our politicians remain thoroughly resistant to even the most sophisticated and subtle approaches.

It is critical we do not let fear of foreign interference undermine stakeholder engagement or stoke community division. Were this to happen, it would perversely have the same corrosive impact on our democracy as foreign interference itself.

This year—a federal election year—we need to be particularly on guard against foreign political interference.

I can confirm that ASIO recently detected and disrupted a foreign interference plot in the lead-up to an election in Australia. I'm not going to identify the jurisdiction because we are seeing attempts at foreign interference at all levels of government, in all states and territories.

But it is important to explain what political interference actually looks like.

This case involved a wealthy individual who maintained direct and deep connections with a foreign government and its intelligence agencies. This agent of interference has roots in Australia but did the bidding of offshore masters, knowingly and covertly seeking to advance the interests of the foreign power and, in the process, undermine Australia's sovereignty.

I'll call this person 'the puppeteer', although it's important to remember that while the puppeteer pulled the strings, the foreign government called the shots.

The puppeteer hired a person to enable foreign interference operations and used an offshore bank account to provide hundreds of thousands of dollars for operating expenses. Secretly shaping the jurisdiction's political scene to benefit the foreign power was considered a key performance indicator. It was like a foreign interference start-up.

The employee hired by the puppeteer began identifying candidates likely to run in the election who either supported the interests of the foreign government or who were assessed as vulnerable to inducements and cultivation. The employee used existing relationships with politicians, staffers and journalists to select potential targets, without revealing the secret intent, the foreign connection or the puppeteer's involvement.

The puppeteer and the employee plotted ways of advancing the candidates' political prospects through generous support, placing favourable stories in foreign language news platforms and providing other forms of assistance. They investigated hiring political consultants, advertising agencies and PR specialists to help individual campaigns. The aim was not just to get the candidates into positions of power, but also to generate a sense of appreciation, obligation and indebtedness that could subsequently be exploited.

The political candidates had no knowledge of the plot. Even if the plan had proceeded, they would not have known who was pulling the strings. The puppeteer used the employee as a cut-out. This deliberate deceit and secrecy about the foreign government connection is what took the case into the realm of foreign interference.

At this point, ASIO acted. Our intervention ensured the plan was not executed, and harm was avoided.

It's impossible to know exactly what would have happened without ASIO's disruption but I can offer an informed scenario. Some of the candidates get elected. The puppeteer's employee then recommends they hire certain other associates as political staffers. These people are also agents or proxies of the foreign government, and will try to influence the politician, shape decision-making and help identify other political figures who can be influenced and recruited. Down the track, the new parliamentarians might be asked for information about the party's position on defence policy, human rights, foreign investment or trade. This information will be sent to the foreign power without the knowledge of the parliamentarian. At some point, the politicians might be prevailed upon to vote a particular way on a contentious issue, or lobby colleagues to vote a certain way.

I know that this is how it plays out because we've seen it happen in situations where we uncovered the foreign interference at a later stage. These cases are much more serious.

This is why ASIO's role is crucial. We and our partners use a suite of measures to disrupt foreign interference plots. The tools include defensive briefings to potential victims; interviews of perpetrators and other targeted intelligence activities; visa cancellations if we are dealing with foreign nationals and, of course, law enforcement action.

The first and most effective defence against all forms of foreign interference is awareness. Know who you are dealing with and why. That's why I've given you a level of detail that we would normally not reveal in public. I want to improve your understanding of what foreign interference is—and, just as importantly, what it is not. The case study I've described makes it clear that foreign interference in our political system is far removed from lobbying, diplomacy or other open and transparent attempts to influence decision-making.

And as I mentioned earlier, I do not want misunderstandings about foreign interference to undermine democratic processes, community engagement or our multicultural society, which I firmly believe is a national asset.

The perpetrators of foreign interference carefully hide their true motivations. But that does not mean politicians are powerless to protect themselves.

The instincts, values and transparency that guide other elements of political engagement are powerful shields against foreign interference. If a supporter wants to provide significant levels of assistance or install a certain staffer in your office, do your due diligence. If business operators want to donate significant resources to your campaign, ask what's in it for them. If a media proprietor promises unlimited positive coverage, query their motives.

To be clear, I'm not suggesting people should reflexively turn down these types of assistance; just that they should be aware of the risks, pose the appropriate questions, and be transparent and accountable about what's received. And, most critically, stay alert to the backers calling in their favours by asking for something that conflicts with Australia's interests.

Security is a shared responsibility.

That's the message I want to leave you with tonight.

I want to assure you of two things: good security is achievable, and good security works.

I find it infuriating when companies say they were done over by an adversary so powerful there was no way to defend against it. That's what I call the Borg defence—'resistance is futile'.

In my experience, resistance is rarely futile.

Certainly, in the cyber field, the overwhelming majority of compromises are foreseeable and avoidable.

While some of these are seriously damaging, many others that are breathlessly called 'cyber-attacks' in the media are not compromises at all—they are reconnaissance missions; if the digital doors are locked, the intruder moves on and tries somewhere else.

At the same time, I'm the first to admit ASIO is not all-seeing or all-knowing—we don't want to be—and while ASIO is part of the answer to the challenges I've outlined, we are not the whole answer.

The acceleration of radicalisation, online propaganda and misinformation, single-issue extremism and minors embracing violent extremism all require a whole-of-government, whole-of-system and whole-of-nation approach.

That's why teamwork is critical.

Our work with law enforcement, the national intelligence community, Home Affairs and our international counterparts is well known—all of you are represented in the room tonight and I want to thank and commend you for being such effective mission enablers, leaders and force multipliers.

But ASIO can do more. The scale and scope of Australia's adversaries requires a broader approach to security intelligence, its influence and impact.

The threat environment demands we take our engagement to a new strategic level. It's what we call 'hardening the environment'; making our economy, institutions and political system more difficult and resilient targets for those seeking to undermine them.

I started this address with a personal admission, so I might as well conclude with one, too.

The Director-General of Security is not always the most welcome visitor. All too often when I knock on a door the person who opens it looks like they are thinking, 'Uh oh—here comes the bad news.'

It's time to improve that.

Obviously, ASIO will continue to identify and communicate threats, but I want to put more emphasis on what you can do about them.

How you can protect your people, places, technology and information.

How a good security strategy addresses physical security, IT security and personal security.

As I said before, good security is achievable, and good security works.

The threats facing Australia are serious, but not insurmountable. Our adversaries are sophisticated, but not unstoppable.

In all the case studies I presented this evening—the online radicalisers, the teenage extremists, the nation-state conducting political interference—in all of them, the adversary made a mistake that brought its activities to ASIO's attention and led to the threat being mitigated.

And just in case our adversaries are listening, I should point out that you don't need to make a mistake to come to our attention. ASIO can catch you even if your tradecraft is perfect. I'll back my people any day.

ASIO will always play its part. We will protect Australia's security and safeguard its sovereignty. We will detect and defeat Australia's adversaries, and we will work with our partners to defend our nation's interests.

Thank you.

© Copyright 2021 Disclaimer Privacy Copyright Accessibility Sitemap and Feeds

Back to top